2001

NASA/ASEE SUMMER FACULTY FELLOWSHIP PROGRAM

MARSHALL SPACE FLIGHT CENTER
THE UNIVERITY OF ALABAMA IN HUNTSVILLE

AN OVERVIEW OF PRA WITH APPLICATIONS TO AEROSPACE SYSTEMS

Prepared by:	Sharon E. Navard
Academic Rank:	Assistant Professor
Institution and Department:	The College of New Jersey Department of Mathematics & Statistics
NASA/MSFC Program:	2nd Generation Reusable Launch Vehicle (RLV)
MSFC Colleague:	Fayssal M. Safie

Introduction

Probabilistic Risk Assessment (PRA) is a systematic process for evaluating the probabilities and consequences of undesirable events that can occur in a process or system along with providing a measure of the uncertainty associated with these probability estimates. In the past it was looked at with suspicion by many at NASA, perhaps because of bad experiences with unsuccessful quantitative methods during the Apollo era, but since the *Challenger* accident NASA has mandated that it be used, and it has been very successful. With NASA's new "faster, better, cheaper" philosophy, it is vital that a tool be in place that can help to achieve these goals in the reliability area. This paper describes the history of PRA, gives examples of its aerospace applications to date, and gives suggestions for how it can be used in the future, both for space shuttle upgrades and for totally new technologies such as the 2nd Generation Reusable Launch Vehicle.

A Brief History of PRA

NASA's earliest attempts at probabilistic risk assessment were somewhat less than successful. Early Apollo program estimates of the probability of a successful moon landing mission were as low as 0.2, whereas the observed success rate was 6 out of 7, or 0.86 (Stamatelatos, 2001). Perhaps for this reason NASA basically abandoned quantitative techniques and switched to qualitative methods, most notably the Failure Mode and Effects Analyses (FMEA) with their associated Critical Items List (CIL). The FMEA/CIL process was so successful that it became entrenched within NASA, and quantitative methods were not seriously used even during the development of the space shuttle and into the early eighties.

In the meantime, during the sixties and seventies, the nuclear power industry began to have an increasingly bad public relations problem. For a discussion of the reasons why, see Fragola (1996). The industry designed safety into the plants using a qualitative method called design basis accidents (DBAs) which was similar to NASA's FMEA/CIL process, but it provided no estimate of the probability of a plant accident. Responding to public pressure to quantify the reliability of nuclear power plants, a quantitative study was conducted and published in Rasmussen (1975). This study, which was based on a combination of fault trees and event trees, was the basis of modern probabilistic risk analysis.

Prior to the *Challenger* accident in January 1986, no significant quantitative risk assessments were done at NASA. Quantitative estimates based on expert judgment were used, giving extremely optimistic failure probabilities on the order of one in several thousand. In the aftermath of *Challenger* when NASA's risk pronouncements were studied in fine detail, both the Rogers and Slay Commissions (Rogers et. al. 1986 and Slay et. al. 1988) strongly recommended that NASA improve its quantitative approach. Two proof-of-concept studies were commissioned, one on the Shuttle Auxiliary Power System and the other on the Main Propulsion Pressurization Subsystem (Slay, et al., 1987, and Plistiras et al., 1988).

Not surprisingly, the first comprehensive PRA of the shuttle was conducted for the launch of the *Galileo* probe (Buchbinder, 1989). The spacecraft contained plutonium fuel, and there was great concern that a launch accident would be an environmental disaster. This study, which covered

only the ascent phase, estimated failure probabilities between 1/350 and 1/18, with a mean of 1/78. The *Galileo* study was updated in 1993 (SAIC 1993), and a PRA of the shuttle in all phases was completed in 1995 (Fragola, et. al., 1995). Finally, in 1996 NASA conducted its own study to develop a shuttle PRA model. The model developed uses the Quantitative Risk Assessment System (QRAS) which was developed by NASA. For a more complete history of PRA, see Fragola (1996) and Paté-Cornell & Dillon (2000).

The PRA Process

Probabilistic Risk Assessment is a process that follows a quantitative approach to determine the risk of a top undesirable event and the associated uncertainty arising from inherent causes. It is not a specific technique, but rather an adaptable process that can be modified to fit different situations. However, there are some characteristics that all PRAs have in common. It requires the identification of the top level events of interest and the initiating events that can lead to them. The system must be diagrammed, usually using event trees and fault trees, and probabilities must be determined as well as their associated uncertainties.

A PRA begins by defining the goals and objectives of the study, and the end states of interest. For example, the goal might be to determine what can go wrong, how likely these things are to happen, how uncertain the results are, and how the risks can be mitigated. For the 2nd Generation RLV, end states of interest might be Loss of Mission, Loss of Vehicle, or Loss of Crew.

Once the objectives are known, it is necessary to determine the initiating event categories. To do this, it is necessary for the analyst to be extremely familiar with the system. A preferred tool for identifying the initiating events is a Master Logic Diagram (MLD). The MLD is a top-down procedure that begins with an end state and works down, with each lower step identifying events that are necessary but not sufficient to produce the higher level event. The top levels are functional failures, and the lower levels are subsystem and component levels. The hierarchy continues until groups of initiating event categories are determined that have the same system response.

For each initiating event identified, accident scenarios are then developed. This can be done with event sequence diagrams (ESDs) or event trees. The ESD is an inductive bottom-up procedure that begins with an initiating event and is developed by asking the question "What could happen next?" It ends with the top level events. The ESD can be quantified by converting it to an event tree, where each node of the tree has an associated probability of occurrence.

The compliment to the event tree is the fault tree, which is a deductive top-down procedure. It begins with the end state and works down by asking the question "How could this event have happened?" Fault trees and event trees are used together to delineate the necessary and sufficient conditions for the top level events to occur. They form the basis of the Boolean algebraic equations used to find the probabilities and uncertainties of the top events (Maggio, 1996).

Before reliabilities and uncertainties can be calculated, it is necessary to collect data. The data can be from previous operational experience, test data, handbooks, design engineering, or expert experience. Often the data is scarce, and when this is the case, Bayesian analysis is applied. The

final reliabilities are usually expressed as the 5th, 50th, and 95th percentiles of the Bayesian posterior distributions.

Aerospace Applications of PRA

Several aerospace applications of PRA have already been mentioned—in particular, the proof-of concept studies, the *Galileo* study and its update, the PRA of the space shuttle in all phases, and the development of QRAS. There have been other aerospace applications. PRA has been used to assess the safety of wind tunnels at both Langley Research Center and Ames Research Center. An external maintenance study of Space Station *Freedom* led to design changes to reduce the predicted maintenance load (Fisher and Price et. al., 1990). The *Cassini* probe also had a nuclear fuel, but it was launched on a Titan IV rocket and hence required its own PRA prior to launch (PRC, 1994). QRAS is now being used successfully to evaluate upgrades of space shuttle propulsion elements (Safie, 1998).

PRA can also be a useful tool for a system that is in the design phase. It is being used in the Space Exploration Initiative Program (Buchbinder, 1993) as well as in the Space Launch Initiative, or 2nd Generation Reusable Launch Vehicle Program. The 2nd Gen program is trying to apply PRA in selective areas such as engines and ground operations, where enough design information is available to decompose the system. More in-depth PRA studies will be developed at later design phases of the program.

While at first glance it might seem that it is impossible to do PRA in the earliest design stages of a new system, it can actually be quite useful. The very process of systematically outlining the design options and studying the tradeoffs can be enlightening to design engineers. New design options might actually be revealed in this process, while others may be shown to be unfeasible. It can help prevent the program from being sidetracked by interesting sounding alternatives that clearly will not work.

Conclusions

PRA has proven to be a valuable tool for NASA in designing safe and reliable vehicles. Besides providing a method to calculate the reliability of an existing system, it also provides a means of doing sensitivity analyses and trade studies. The QRAS model is making it easier to do these analyses for space shuttle upgrades. Finally, the PRA thought process can be useful in helping to choose the best designs and systems for the 2nd Generation Reusable Launch Vehicle.

References

Buchbinder, Ben, "Independent Assessment of Shuttle Accident Scenario Probabilities for the Galileo Mission", Vol. 1, April 1989, NASA/HQ Code QS, Washington, D.C., 20546.

Buchbinder, Ben, "Risk Management for the Space Exploration Initiative", AIAA 93-0377, 31st Aerospace Sciences Meeting & Exhibit, Reno, Nevada, January 11-14, 1993.

Fisher, W. F., and Price, C. R., et. al., "External Maintenance Task Team", Final Report, Vol. 1, NASA/JSC, Houston, Texas, 1990.

Fragola, Joseph R., et. al., "Probabilistic Risk Assessment of the Space Shuttle: A study of the Potential of Losing the Vehicle During Nominal Operation Volume 1: Final Report", SAIC, February 28, 1995.

Fragola, Joseph R., "Space Shuttle Program Risk Management", 1996 Proceedings of the Annual Reliability and Maintainability Symposium, pp. 133-142.

Maggio, Gaspare, "Space Shuttle Probabilistic Risk Assessment: Methodology & Application", 1996 Proceedings of the Annual Reliability and Maintainability Symposium, pp. 121-132.

Paté-Cornell, Elisabeth, and Dillon, Robin, "Probabilistic Risk Analysis for the NASA Space Shuttle: A Brief History and Current Work", submitted to *Reliability Engineering and System Safety*, April 2000.

Plistiras, J. et. al., "Space Shuttle Main Propulsion Pressurization System Probabilistic Risk Assessment," Final Report, Lockheed Corp., Palo Alto, CA, 1988.

PRC, "Analysis Methodology Report: Titan IV *Cassini* RTG Safety Databook: Final", submitted to Martin Marietta Space Launch Systems, September 16, 1994.

Rasmussen, Norman C., "Reactor Safety Study—An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", WASH-1400, U.S. Nuclear Regulatory Commission, October 1975.

Rogers, W. et. al., "Report of the Presidential Commission on the Space Shuttle *Challenger* Accident", Washington, D.C., 1986. (See especially II-F, "Personal Observations of Reliability of Shuttle, Feynman, R.)

Safie, Fayssal M., "An Overview of Quantitative Risk Assessment of Space Shuttle Propulsion Elements", PSAM4 Probabilistic Safety Assessment and Management, 1998.

SAIC, "Probabilistic Risk Assessment of the Space Shuttle Phase 1: Space Shuttle Catastrophic Failure Frequency Final Report", 1995.

Slay, et. al., "Space Shuttle Risk Assessment Proof-of-Concept Study, Auxiliary Power Unit and Hydraulic Power Unit Analysis Report," McDonnell Douglas Corp., December 18, 1987.

Slay et. al., "Post-*Challenger* Evaluation of Space Shuttle Risk Assessment and Management", National Research Council Report, National Academy of Sciences, National Academy Press, Washington, D.C., January 1988.

Stamatelatos, Michael, et. al., "Probabilistic Risk Assessment Workshop for NASA Managers and Practitioners," presented at NASA Headquarters, April 2-5, 2001.